Datorer för underhåll och övervakning av komponenter i automationssystem

Dan Forsström

Examensarbete

Informationsteknik

2012

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informationsteknik
Identifikationsnummer:	3791
Författare:	Dan Forsström
Arbetets namn:	Datorer för underhåll och övervakning av komponenter i automationssystem
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	Fortum Power and Heat Ab

Sammandrag:

I examensarbetet undersöks olika möjligheter för underhåll och övervakning av komponenter i automationssystem. Beställaren betonade att den fungerande miljön bör vara enkel att upprätthålla, att säkerheten är en viktig faktor och att det skall vara möjligt att få data sparat externt.

Examensarbetet består av en teoretisk och en praktisk del. I teoridelen beskrivs virtualisering som är tekniken i den praktiska delen, samt verktygen och hurudana virtualiseringsmöjligheter som erbjuds. Den praktiska delen beskriver de virtualiseringsmöjligheter som har testats och problem som uppstått samt hur de är lösta. Den virtualiseringsmetod som fungerade och konceptets vidareutveckling beskrivs också.

Applikationsvirtualisering och full virtualisering har testats. Applikationsvirtualiseringen orsakade licensproblem i processkomponenternas programvaror. Problemen gick inte att åtgärda och därför slopades alternativet. Problem uppstod också vid full virtualisering. Några processkomponenters programvaror var versionskänsliga. Problemen gick att lösa med hjälp av rätt version av virtualiseringsverktygen. De virtuella maskinerna måste konfigureras innan första uppstarten för att serieporten skall bli tillgänglig och att dataöverföring skall bli möjlig. Både de fysiska och de virtuella maskinerna är härdade och säkrade.

Nyckelord:	virtualisering, ThinApp, applikationsvirtualisering, Workstation, VMware, dator, härdning, programpaket, hårdvara
Sidantal:	47
Språk:	Svenska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	Information Technology
Identification number:	3791
Author:	Dan Forsström
Title:	Computers for Maintenance and Monitoring of Automation System Components
Supervisor (Arcada):	Göran Pulkkis
Commissioned by:	Fortum Power and Heat Oy

Abstract:

The aim of the thesis was to investigate ways to maintain and monitor automation system components. The orderer emphasized that the working environment should be easy to maintain, that security is an important factor and that it should be possible to get data stored externally.

The thesis consists of a theoretical and a practical part. The theoretical part describes virtualization which is the technology in the practical part, the tools and what kind of virtualization opportunities is offered. The practical part describes the virtualization capabilities that have been tested, problems identified and how they are solved. The virtualization method that worked and further development of the concept is also described.

Application virtualization and full virtualization has been tested. Application virtualization caused component software license issues. The problems could not be solved and therefore application virtualization was abandoned. Also in full virtualization occurred problems. Some software components were version sensitive. The problems were solved by using the correct version of the virtualization tools. The virtual machines must be configured before the first boot, in order to get serial port access and to make data transfer possible. Both the physical and the virtual machines are hardened and secured.

Keywords:	virtualization, ThinApp, application virtualization, Workstation, VMware, computer, hardening, software, hardware
Number of pages:	47
Language:	Swedish
Date of acceptance:	

INNEHÅLL

Figurer

FÖRORD

Detta arbete har gjorts för Fortum Power and Heat Ab, Lovisa kraftverk. Jag vill tacka Fortum för examensarbetsmöjligheten. Framför allt vill jag tacka min handledare, avdelningschefen för Process IT, Robert Valkama, som gjorde hela projektet möjligt. Jag vill också tacka systemexperten Mika Torvinen för hans goda råd och idéer.

Jag vill tacka min handledare vid Arcada, Göran Pulkkis, som har gett mig stöd och råd under skrivprocessen.

Tack till alla som har hjälpt och stött mig under studietiden.

Lovisa 31.7.2012
Dan Forsström

1 INLEDNING

Detta examensarbete är gjort som ett projekt för Fortum Power and Heat Ab. Utgångspunkten är att ta reda på olika möjligheter för att kunna upprätthålla och övervaka automationssystems komponenter. Beställaren betonade att den fungerande miljön bör vara enkel att upprätthålla, att säkerheten är en viktig faktor och att det skall vara möjligt att få data sparat externt. Projektet är utfört genom testning av olika virtualiseringsmöjligheter.

1.1 Målsättning

Problemet bakom hela projektet är att ett automationssystems livslängd är ungefär 20 år, medan en dator med en specifik hårdvara har en livslängd på ungefär fem år. Syftet med detta projekt var att utreda om det är möjligt att skapa en miljö var man kan köra olika processkomponenters programvaror. Ett syfte var också att utreda på basen av testning vilka olika sätt är möjliga eller är det överhuvudtaget möjligt att bilda en fungerande miljö. Arbetets målsättning var att skapa en prototyp (proof of concept) av en eller flera fungerande miljöer var man kan köra komponenternas programvaror. Miljön skulle vara härdad och kunna hantera programvaror, uppdateringar samt virusskydd.

Examensarbetets skriftliga del är indelad i en teoretisk och en praktisk del. Den teoretiska delen består av en överblick på virtualisering och hurudana möjligheter som erbjuds samt vilka verktyg som använts. Den praktiska delen beskriver hur projektet var förverkligat samt projektets resultat och slutsatser.

1.2 Begränsningar

Examensarbetet kommer inte att omfatta underhåll av den möjliga prototypen. På grund av Fortums säkerhetspolitik beskrivs inte ”Group Policy”-inställningar eller andra specifika inställningar. Arbetet fokuserar på utveckling av olika virtualiseringsmiljöer. I detta projekt testas endast VMware-virtualiseringsverktyg.

2 VIRTUALISERING

Virtualisering är en teknisk innovation som gör det möjligt att installera olika tjänster på fysiska enheter så att de i framtiden inte är beroende av hårdvaran. Virtualisering beskriver sättet hur virtuell hårdvara separeras från den fysiska hårdvaran genom att efterlikna hårdvara med hjälp av virtualiseringsmjukvara (Figur 1). En virtuell dator är egentligen en datafil eller datamapp, inte en fysisk dator, den kan kopieras och flyttas till en annan dator precis som alla andra filer. Datorn som den virtualiserade tjänsten har flyttats till behöver endast ha virtualiseringsmjukvaran installerad för att kunna köra tjänsten. (Burford. 2008) Virtualisering används nästan på alla områden inom informationsteknik. Virtualisering används t.ex. inom försäljning, undervisning, testning och nätverk.

2.1 Historia och nutid

Virtualiseringstekniken är ingen ny sak, utan man har känt till de grundläggande principerna redan en längre tid (Mäntylä. 2008). På 1960-talet började IBM utveckla virtualisering av stordatorerna genom att logiskt dela upp dem i virtuella maskiner för att kunna utnyttja all hårdvara. Stordatorerna var mycket dyra på den tiden och därför började man leta efter olika lösningar för att kunna fullt utnyttja de egna resurserna. Under 1980- och 1990-talen slopades virtualiseringstekniken på grund av att desktopdatorer, servrar och de nya operativsystemen Windows och Linux tog över. Underhåll av dessa system, infrastrukturernas kostnader och otillräckligt katastrofskydd har lett till virtualisering av de nya systemen för att kunna utnyttja alla resurser samt minska på kostnaderna. VMware utvecklade virtualiseringen för x86-system år 1999. Virtualiseringen tog fart vid sekelskiftet då VMware introducerade virtualisering på x86-system. (InfoBarrel. 2010)

Virtualiseringen är också en viktig del inom grön IT. Grön IT försöker gynna miljön genom att förbättra energieffektiviteten samt sänka utsläpp av växthusgaser. Med hjälp av virtualisering kan datacenter köra flera virtuella servrar på en kraftfull server och på så sätt används det mindre elektricitet för att driva samma mängd servrar. (Murugesan. 2008, 29)

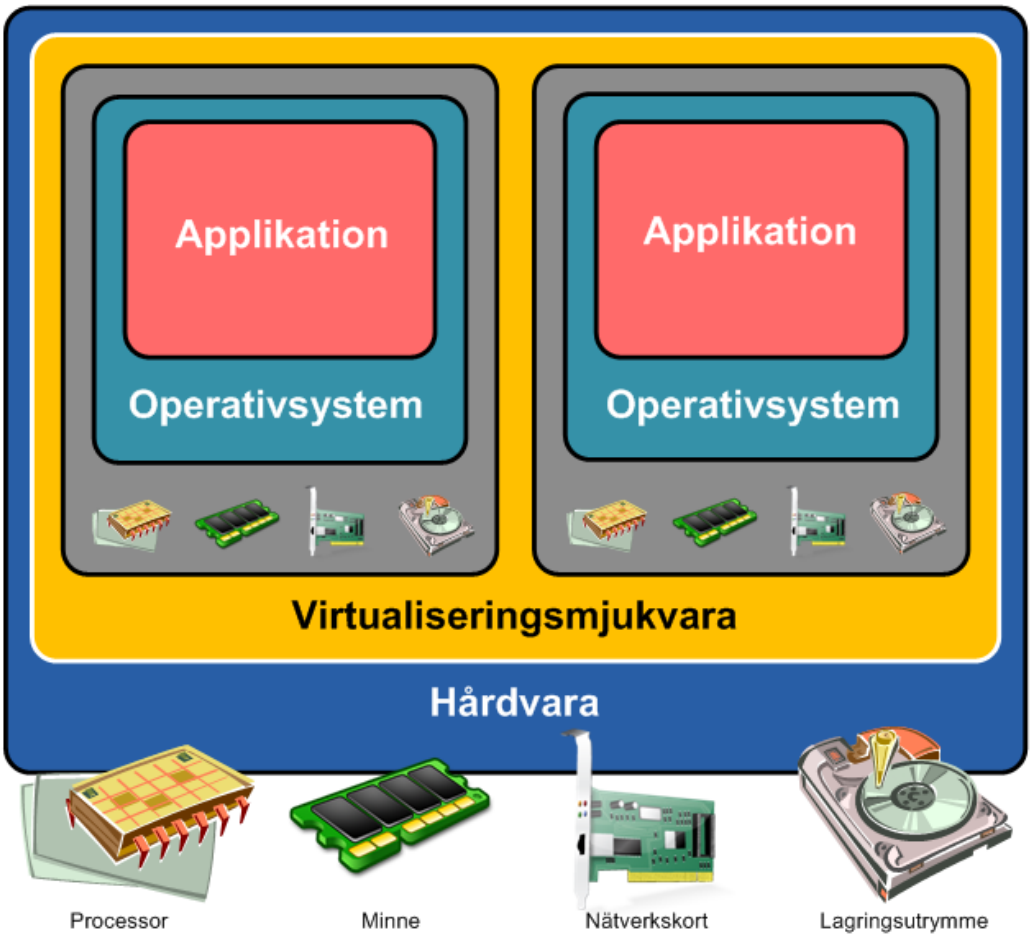
2.2 Fördelar med virtualisering

De flesta företag försöker dagligen hitta olika sätt att spara pengar på och strävar efter att kunna göra mer med mindre resurser. På det här sättet sparar företaget elektricitet och arbetskraft. Därför har virtualisering av programvaror och servrar ökat i företag.

Genom att virtualisera program och operativsystem gör man dem oberoende av en specifik hårdvara, istället fungerar de virtuella lösningarna på nästan all hårdvara som har samma virtualiseringsprogram installerat. På det här viset blir t.ex. ett operativsystem inte bundet till en specifik hårdvara och kan därför användas i framtiden fast hårdvaran uppdateras.

Virtualisering baserar sig på logisk partitionering. Med logisk partitionering kan man köra flera virtuella maskiner på en och samma hårdvara och tillika är alla virtualmaskiner isolerade från varandra. Ifall det inträffar ett fel på en virtuell maskin kommer det inte att påverka de andra. Den här tekniken effektiverar också kopiering och installering av virtualmaskiner. (Ribière. 2008, s. 1546)

Det är möjligt att köra olika operativsystem på samma fysiska enhet. Att köra äldre program på ny hårdvara är möjligt med hjälp av virtualisering. Orsaken till detta är att man kan konfigurera och skapa en virtuell miljö som stöder den äldre programvaran. Virtualiseringsmjukvaran hanterar den äldre programvaran genom att från den fysiska hårdvaran skapa virtuell hårdvara som lämpar sig för den äldre programvaran. (Ribière. 2008, s. 1546)



Figur 1. Virtuell hårdvara är separerad från fysisk hårdvara genom att efterlikna hårdvaran med hjälp av virtualiseringsmjukvara.

2.3 Nackdelar med virtualisering

Virtualisering har många fördelar men också många nackdelar. Det går inte att virtualisera allting, det finns programvara och hårdvara som på grund av olika skäl inte går att virtualisera, t.ex. hårdvarubegränsningar. Det sägs att man gör besparningar genom att virtualisera, men inte alltid. Säkerheten gällande virtualmaskiner och servrar är inte alltid så lätt att hantera.

En virtualmaskin når aldrig en fysisk dators prestanda. Det har varit svårt att få tillräcklig processorkraft för att kunna köra virtualmaskinen på den fysiska datorn, så att det inte skulle uppstå latens. Nuförtiden när virtualisering blivit populärare har

processortillverkarna Intel och AMD utvecklat och infört tekniker som främjar virtualisering. (Ribière. 2008, s. 1546)

Begränsad hårdvara är ett annat problem då man skall virtualisera. Enligt Alain Ribière känner virtualmaskiner till den vanligaste kringutrustningen såsom USB och olika SCSI. Detta kan vara ett problem då man kör en virtualmaskin på en fysisk dator som är kopplad till en komponent via en specialport. Problemet kan vara att virtualmaskinen inte kommer åt specialporten. Oftast beror detta på virtualiseringsmjukvaran som inte stöder specialporten och kan inte därför koppla den till virtualmaskinen. (Ribière. 2008, s. 1546)

Genom virtualisering kan man minska på resurser, men direkta kostnadsbesparingar gällande programvarulicenser lyckas sällan. Orsaken är den att oavsett om ett program körs på en virtuell maskin eller på en fysisk dator gäller samma principer för användarlicenser. Det finns gratis virtualiseringsmjukvara på marknaden men den är främst avsedd för hemmabruk. I framtiden, när efterfrågan stiger, är det möjligt att virtualiseringsprogrammen blir billigare. (Hämäläinen. 2007)

2.4 Typer av virtualisering

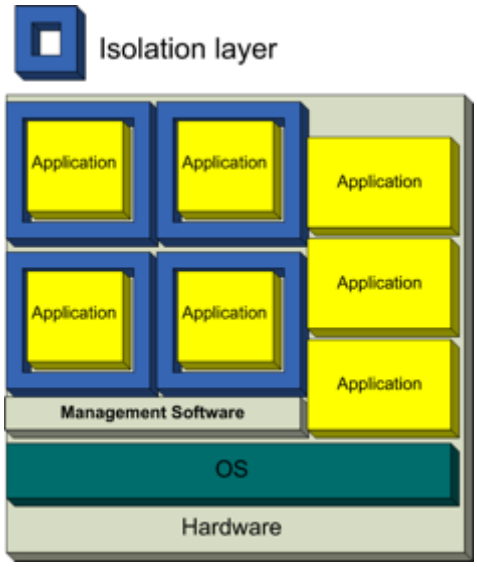
Virtualisering kan delas i olika typer. De tre huvudtyperna är ”Software as a Service”, ”Platform as a Service” och ”Infrastrucutre as a Service”. Dessa termer härstammar från cloud computing, men eftersom cloud computing baserar sig på virtualisering, kan man använda sig av dessa termer inom virtualisering. ”Platform as a Service” och ”Infrastructure as a Service” bygger på virtualiseringsteknikerna paravirtualisering och full virtualisering.

2.4.1 Software as a Service

”Software as a Service” (SaaS) betyder att slutanvändaren kan köra en applikation oberoende av vilket operativsystem som används. Applikationen kan vara på den lokala datorn eller så körs den i ett webbgränssnitt via Internet. Den som använder

applikationen kan inte kontrollera den underliggande infrastrukturen, endast användarspecifik konfiguration är möjlig. (Hoefer & Karagiannis. 2010, s. 1346)

Liz van Dijk berättar i sin artikel att applikationsvirtualisering är svår att definiera på grund av termens breda betydelse. Applikationerna är isolerade från varandra, i sina egna paket, som fungerar på egna operativsystem (Figur 2). Eftersom ett paket är praktiskt taget en egen miljö, behöver det inte några speciella inställningar för att fungera korrekt. Detta möjliggör enkel distribution av applikationerna till andra maskiner samt en differentierad miljö för varje applikation. (Dijk. 2008)



Figur 2. Applikationerna är isolerade till en egen miljö. (Dijk. 2008)

Systemadministratörer letar ständigt efter nya sätt för distribuering av programvara. Oftast orsakar stora system med många klienter problem vid distribution av programvara. I detta fall är också programvarans licensering svårt. Genom att virtualisera programvaran kan den användas i vilken situation som helst, i sin egna specifika miljö och kan hanteras centrerat. (Dijk. 2008)

Applikationsvirtualisering är ett alternativ då man försöker få äldre programvara att exekvera på en ny dator. Oftast är problemet det att företag är i något skede tvungna att investera i nya datorer och på så sätt uppdatera systemen. Ett problem som oftast uppstår i det här skedet är att man inser att man använder programvara som inte stöder

nyare operativsystem eller hårdvara. Problemet kan lösas genom att virtualisera programvaran. Först installerar man virtualiseringsmjukvaran på det underliggande operativsystemet som hårdvaran stöder. Sedan skapar man en virtuell dator med det operativsystem som applikationsprogramvaran stöder. Till sist installeras applikationsprogrammet. Applikationsvirtualiseringsmjukvaran isolerar programvaran i sin egen miljö. Programvaran tror att den körs på rätt operativsystem, men egentligen blir den virtualiserade programvaran en exekverbar fil som kan köras nästan var som helst. Programmets virtualisering behövs bara göras en gång och kan sedan lätt delas ut t.ex. genom kopiering (Figur 2).

2.4.2 Platform as a Service

”Platform as a Service” (PaaS) erbjuder en mjukvaruinfrastruktur var användaren kan köra egna program och lämpar sig därför bra som testmiljö. Ifall någonting går fel eller systemet kraschar är det lätt att ta i bruk en ny plattform utan att den fysiska datorn skadas. En plattform är ett paket som har ett operativsystem färdigt installerat, men det finns också paket med både operativsystem och annan mjukvara färdigt installerade. Plattformens användare kan använda sig av den underliggande hårdvaran, såsom nätverk och lagring, men kan inte kontrollera den för de ligger ytterom plattformen. (Hoefer & Karagiannis. 2010, s. 1346)

2.4.3 Infrastructure as a Service

”Infrastructure as a Service” (IaaS) erbjuder själva hårdvaran som används för att kunna skapa nya virtualplattformer. Genom att virtualisera en hårdvara kan flera användare använda sig av samma hårdvara. På det här sättet får man mera ut från t.ex. en servers hårdvara samt man behöver endast investera en hårdvara. Den här typen av virtualisering gör det möjligt att skapa ett internt (privat) moln, t.ex. inom ett företag var man kan erbjuda hårdvara. Ifall företaget inte har möjlighet att virtualisera en viss hårdvara kan en extern (publik) molntjänst kopplas till det privata nätet. Sådana lösningar kallas hybridmoln. (Hoefer & Karagiannis. 2010, s. 1346)

2.4.4 Full virtualisering

Full virtualisering är en virtualiseringsteknik som används för att skapa en viss typ av virtuell miljö genom att fullständigt avbilda den underliggande hårdvaran. I denna virtuella miljö kan man exekvera alla program som går att köra direkt på hårdvaran samt man kan installera nästan vilket operativsystem som helst.

Den här tekniken använder en speciell typ av programvara som kallas en hypervisor. Hypovisorn interagerar direkt med fysiska datorns processor och diskutrymme. Den fungerar som en plattform för de virtuella datorernas operativsystem. Hypervisorn isolerar varje virtuell dator så att den inte är medveten om eventuella andra virtuella datorer som körs på samma hårdvara. Den fysiska datorns resurser övervakas och styrs av hypervisorn som sedan delegerar resurserna vidare till rätt virtuell dator. Hypervisorn har sina egna behov vilket innebär att den fysiska datorn måste reservera resurser för att kunna köra hypervisor-programmet. Detta påverkar den fysiska datorns prestanda och tillika också de virtuella maskinernas prestanda. (Strickland. 2008)

2.4.5 Paravirtualisering

Paravirtualisering är en virtualiseringsteknik som skapar ett programvarugränssnitt till virtuella maskiner som liknar den underliggande hårdvaran men är inte identisk. Med den här tekniken är det möjligt att ett främmande operativsystem kan agera med värddatorn.

Paravirtualiseringsmetoden är lite annorlunda jämfört med full virtualisering. Skillnaden är den att i ett paravirtualiserat system är de virtuella datorerna medvetna om varandra. Hypervisorn behöver därför mindre resurser för att hantera gästoperativsystem, eftersom varje virtuell dator är medveten om vilka krav de andra virtuella datorerna har lagt på värddatorn. Systemet fungerar som en sammanhängande enhet. (Strickland. 2008)

2.5 Säkerhet

Säkerheten för virtuella maskiner är mycket lik säkerheten gällande fysiska datorer. På en virtuell maskin bör virusskydd, brandmur och uppdateringar vara konfigurerade och

installerade liksom på en fysisk dator. Med hjälp av härdning av den fysiska och den virtuella datorn blir skyddet mot skadliga attacker starkare. Det finns dock säkerhetshot som är unika för den virtuella miljön.

2.5.1 Säkerhetsbrister

Största fördelen med virtualisering är isolering. Isolering kan också vara ett hot ifall isolering inte utnyttjas korrekt. Slarvig isolering eller felaktig konfiguration av åtkomstkontroll kan orsaka attacker mellan virtuella maskiner och virtualiseringsmjukvaran.

VM escape (rymma från virtuell maskin) är ett intrång som kör sin kod på en virtuell maskin. Koden startar oftast upp något program som kan rymma från den virtuella maskinen och kommer på så sätt åt virtualiseringsmjukvaran eller den fysiska datorn. När programmet kommer åt den underliggande datorn, kommer den också åt alla andra virtuella maskiner och får då också kontroll över dem. Den här typen av intrång kan sist och slutligen förstöra hela systemet. (Shengmei et al. 2011 s. 175)

En denial-of-service (DoS) attack försöker göra resurserna otillgänliga för de avsedda användarna. DoS attacker antingen tvingar den utsatta datorn att återställa sig eller så förbrukar de datorns resurser så att datorn inte kan utföra de avsedda tjänsterna. Virtuella maskiner använder samma underliggande hårdvara och då finns det risken att en användare kan införa en DoS attack. En DoS attack i ett virtuellt system går ut på att en virtuell maskin äter upp resurserna så att de andra maskinerna inte fungerar korrekt. (Shengmei et al. 2011 s. 176)

Ett annat hot mot virtuella maskiner är VM sprawl (spridning). VM sprawl orsakas ofta av olämplig administrationspolitik. Denna attack går ut på att antalet virtuella maskiner växer kontinuerligt, medan de flesta nya maskiner inte används och på så sätt äts värddatorns resurser upp. (Shengmei et al. 2011 s. 176)

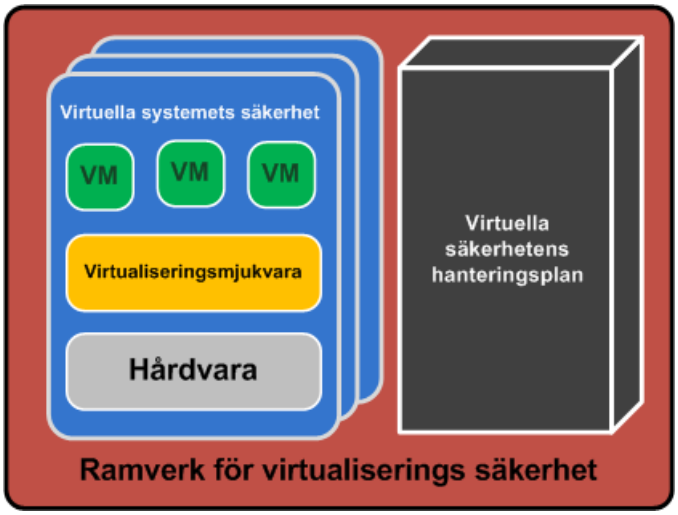
Det viktigaste gällande säkerhet i virtuella maskinernas arkitektur är att komma ihåg att skydda värddatorn mot olika angrepp. Det är viktigt att skydda värddatorn, för att allting

som görs på de virtuella maskinerna registreras i den fysiska datorn. Om värddatorn har blivit utsatt för ett angrepp som t.ex. lyssnar på olika portar kan otroligt mycket information hamna i fel händer. Programmet lyssnar på värddatorns port som alla de virtuella maskinerna också använder, t.ex. nätverksporten. (Shengmei et al. 2011 s. 175)

Begreppet cloud computing baserar sig på virtualisering och är därför utsatt för samma hot som alla andra virtualiserade miljöer. Cloud computing delas in i tre olika slags moln, privata, hybrida och publika. Så länge som ett företag har ett privat moln är datasäkerheten bättre. Ett privat moln uppstår då man virtualiserar inom eget Internet domän. Ifall företaget hyr någon tjänst från det publika molnet till sitt eget privat moln uppstår ett hybridmoln. Publika och hybrida moln upprätthålls delvis eller helt av någon annan och därför skall användaren vara försiktiga med extern datalagring. Den externa datalagringen kan säkras genom att t.ex. använda sig av kryptering.

2.5.2 Hantering

Virtualiseringssäkerhet bör undersökas från två olika aspekter, det virtuella systemets säkerhet och hantering av virtualiseringssäkerhet. Vanligen består det virtuella systemets säkerhet av tre lager. Första lagret är hårdvara, det andra och viktigaste är virtualiseringsmjukvaran och det tredje är de virtuella datorerna. Hantering av virtuell säkerhet går ut på att man har skapat ett schema eller en plan hur man upprätthåller systemet och dess säkerhet (Figur 3). (Shengmei et al. 2011 s. 176)



Figur 3. Ramverket för virtualiseringssäkerhet består av två delar.

För att uppnå ett säkert virtuellt system bör det skyddas med en robust, effektiv och flexibel virtuell systemarkitektur. Förutom den traditionella systemarkitekturen kan man delvis separera säkerhetskontrollen till en virtuell administrationsdator eller helt separera kontrollen av säkerheten till ett eget lager. Genom att använda accesskontroll i den virtuella miljön är det lättare och flexiblare att begränsa resurser för användaren. På det här sättet blir kommunikationen mellan alla lager pålitligare. Det är också viktigt med en virtuell brandmur för att uppnå bättre övervakning av den virtuella miljön. En virtuell brandmur kan skapas på olika sätt. Det kan vara en helt traditionell programbaserad brandmur, en virtuell ”switch” med ytterligare säkerhetsfunktioner eller en process som körs av virtualiseringsmjukvaran. Ett virtuellt system bör kunna motstå attacker som kommer via nätet, därför bör systemet vara utrustat med ett starkt verktyg som förhindrar dessa attacker. Verktyget kallas vIDS (virtual Intrusion Detection System) och det analyserar in- och utgående nätverkskommunikation. (Shengmei et al. 2011 s. 177)

Hantering av den virtuella säkerheten består vanligen av fyra delar, uppdatering, migration, profil (image) och auditionshantering. Uppdateringshantering är viktig för den håller de virtuella maskiner uppdaterade och tillika minskar chansen för attacker. Genom att testa olika kodförändringar kan man sammanställa ett kodpaket, alltså en uppdatering för systemet som körs och installeras t.ex. vid nästa uppstart av datorn. En god plan för migration av virtuella maskiner är viktig, för att kunna undvika attacker under processen samt för att undvika hårdvaruproblem. En virtuell maskin fungerar inte utan sin profil-fil. Därför är det viktigt att säkra denna fil t.ex. vid migration. Med auditering samlar man information från den virtuella maskinen för att senare kunna utreda t.ex. varför den virtuella datorn har kraschat. (Shengmei et al. 2011 s. 177-178)

2.5.3 Härdning

Härdning är en process som gör datorer säkrare. Processen går ut på att man identifierar sårbarheter och på så sätt skapar en kontrollerad miljö (Solomon, Michael.G. 2010, s.269). Med härdning begränsas sårbarheten hos operativsystemet och annan programvara i en dator. En virtuell dator i en fysisk dator är bättre skyddad när den fysiska datorn är härdad och kvarvarande sårbarhet kan ytterligare begränsas med härdning av den virtuella datorn. Datorer eller system har en större sårbarhet ju mer de

är tillåtna att utföra. Genom att t.ex. avlägsna onödiga program, onödiga användarnamn eller onödiga tjänster minskar man möjligheten för externa angrepp.

Virtuella maskiners härdning har några särskilda faktorer som man bör komma ihåg. De viktigaste faktorerna är användning av virusskydd som förstår virtualisering, säkring av virtuella maskiner, säkerhetskopiering och resursbegränsning. (Elmsjö. 2012)

Det lönar sig att använda virusskydd som förstår virtualisering för att spara på resurser. På en virtuell maskin bör man inte använda sig av schemalagda genomsökningar för att dessa är oftast tunga processer och utnyttjar resurser oväntat, då du använder din virtuella maskin till någonting annat. (Elmsjö. 2012)

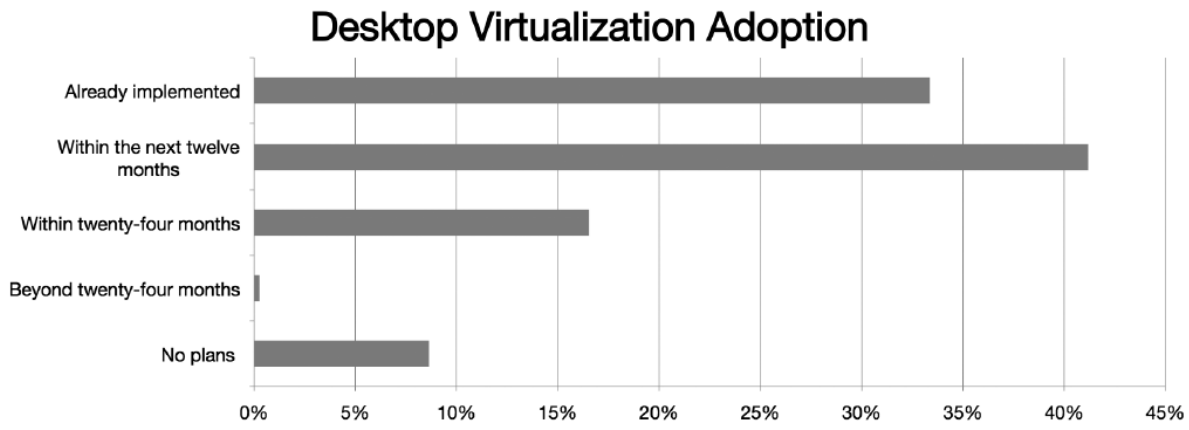
Virtuella maskiner bör vara uppdaterade på samma sätt som en fysisk dator. Det lönar sig att uppdatera operativsystem och allting annat. Magnus Backman kommenterar att en stor fördel man ofta glömmer är att virtuella maskiner väldigt enkelt kan klonas, till exempel för testmiljöer. Det här är mycket bra när man vill testa en ny säkerhetsuppdatering för sin applikation i en ögonblicksbild av en virtuell produktionsmaskin. (Elmsjö. 2012) En profil fil (image) som t.ex. körs vid uppstart av datorn bör konfigureras så att den söker samt installerar uppdateringar förrän den får användas eller så sköts detta manuellt ifall datorn inte är kopplad till Internet.

Säkerhetskopiering och resursbegränsning är också viktiga faktorer. Säkerhetskopiering av virtuella maskiner bör ställas in så att den görs automatiskt med jämna mellanrum. Ifall det körs flera virtuella maskiner på en och samma fysiska dator lönar det sig att begränsa resurserna på ett sådant sätt att virtuella maskiner får exakt den mängd resurser som behövs för att de skall fungera. (Elmsjö. 2012)

2.6 Framtiden är virtuell

Virtualisering kommer att bli allt populärare under de kommande åren. Enligt Citrixs undersökning om desktopvirtualisering har de flesta (91 procent) genomfört virtualisering eller planerat att göra så år 2013 (Figur 4). Ungefär en tredjedel (33

procent) har redan inlett virtualiseringen, medan ytterligare 58 procent planerar att göra så under år 2013. (Citrix Systems, Inc. 2011)



Figur 4. Införsel av virtualisering. (Citrix Systems, Inc. 2011)

Hårdvaran blir ständigt bättre, medan mjukvaru-utvecklingen står på stället. Det finns inte ett operativsystem eller någon applikation som skulle använda all hårdvara i en dator, förutom videoredigering som kräver mera av hårdvaran. För att kunna utnyttja all hårdvara som finns är virtualisering det bästa sättet. Istället för att en hårdvara kör en process så indelas en hårdvara i flera virtuella hårdvaror som kör sina egna processer.

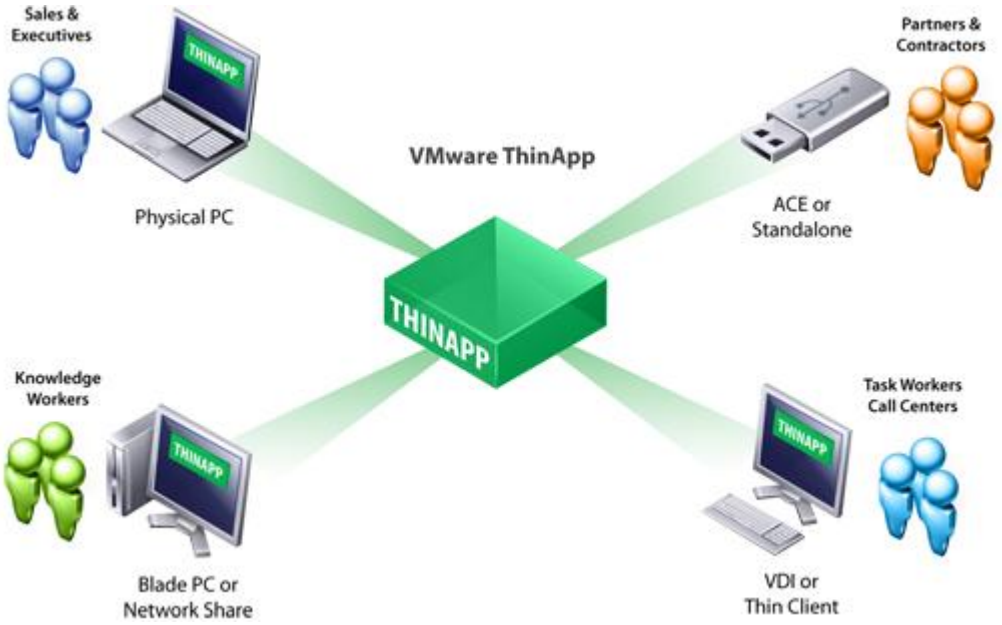
Virtualisering har gjort upprätthållning av äldre system möjlig. Äldre system som t.ex. ett automationssystem, som har en livslängd på 20 år, kräver anpassning av upprätthållningsdatorerna vars livslängd är fem år. Genom att skapa virtuella datorer kan man skapa en miljö som är oberoende av den underliggande hårdvaran och då blir livslängden på upprätthållningsdatorerna längre. Den virtuella miljön är portabel samt lätt att upprätthålla.

3 VERKTYG

Detta kapitel introducerar de verktyg som användes i detta projekt. Med hjälp av dessa verktyg har det varit möjligt att skapa olika testmiljöer för processkomponenternas programvaror.

3.1 VMware ThinApp

VMware ThinApp är ett applikationsvirtualiseringsverktyg. Med detta verktyg kan man isolera program från deras underliggande operativsystem. ThinApp virtualiserar applikationer genom att kapsla in applikationens filer och registerfiler till ett enda paket som kan användas, underhållas och uppdateras oberoende av det underliggande operativsystemet. Därför går det att migrera äldre program till nya system. Virtualiserade applikationer kan köras var som helst samt ökar på flexibiliteten (Figur 5), t.ex. kan applikationen laddas på en USB-sticka för att uppnå maximal bärbarhet. Det är också möjligt att distribuera applikationerna med VMware Horizon Application Manager. (VMware, Inc. 2011a)



Figur 5. ThinApp förenklar applikationsdistribution genom att kapsla in program i bärbara paket som kan distribueras till många ändpunkter. (VMware, Inc. 2011a)

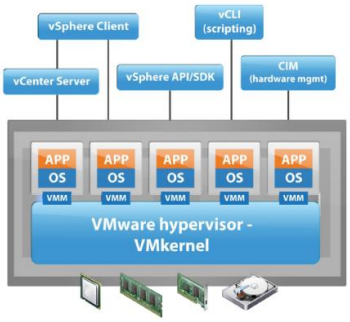
3.2 VMware Workstation

VMware Workstation är en virtualiseringsmjukvara. Fördelen med Workstation är att man kan skapa flera virtuella datorer från samma hårdvara utan extra kostnad. Workstation kör virtuella maskiner i en isolerad och säker miljö. Workstation kan köra flera virtuella maskiner samtidigt på en enda dator. Den fysiska hårdvaran virtualiseras för att den virtuella maskinen skall ha tillgång till en egen hårdvara. Man kan installera vilket operativsystem som helst på den virtuella datorn oberoende av vilket operativsystem som körs på värddatorn. VMware Workstation är en ypperlig programvara då man behöver skapa olika testmiljöer för testning av olika program och inställningar. (VMware, Inc. 2011b)

3.3 VMware vSphere Hypervisor (ESXi)

VMware ESXi är en hypervisor för servrar. Hypervisorn körs oftast direkt på serverns hårdvara utan ett underliggande operativsystem. ESXi skapar ett virtualiseringslager som avskiljer processor-, minnes-, lagrings- och nätverksresurser från den fysiska värden till flera virtuella maskiner. Hypervisorn ESXi är grunden för ett dynamiskt och automatiserat datacenter. ESXi-värden kan nås via olika gränssnitt, t.ex. VMware vSphere Client. (VMware, Inc. 2011b s. 53)

En applikation som körs på en virtuell dator som styrs av hypervisorn ESXi har tillgång till hårdvara men kommer inte åt den underliggande hårdvaran. Hypervisorn ESXi kallas VMkernel. VMKernel tar emot virtuella maskiners förfrågningar från virtuella maskinernas övervakare (Virtual Machine Monitor (VMM)) och gör anrop till den fysiska hårdvaran (Figur 6). (VMware, Inc. 2011c s. 53)



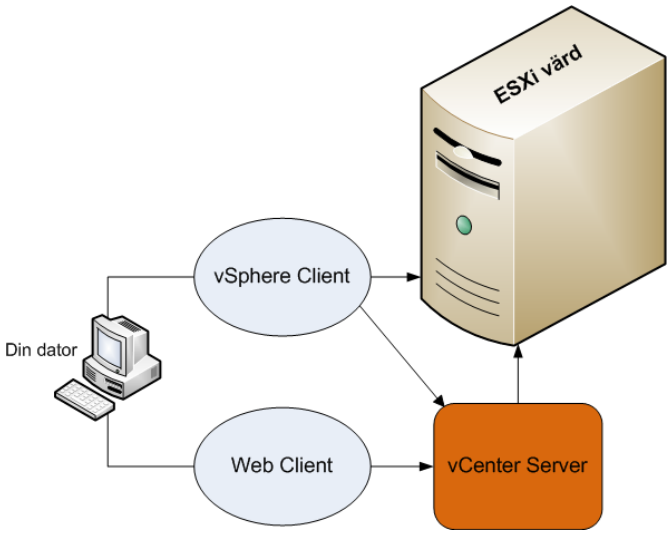
Figur 6. "VMware ESXi"-värdens arkitektur.(VMware, Inc. 2011c s. 53)

3.4 VMware vCenter Server

VMware vCenter Server är ett hanteringsverktyg som möjliggör hantering samt övervakning av virtuella värdar och maskiner från datacentret genom ett enda användargränssnitt. Administratörer har bättre kontroll över molnet. Till vCenter Server kan man koppla flera ESXi-värdar via IP-adresser. Komplexiteten och kostnaderna minskar då en administratör kan kontrollera och uppdatera maskiner på distans. Med hjälp av integrering av Vsphere Update Manager kan uppdateringar och konfigureringar skötas automatiskt. För att komma åt vCenter Server måste man använda sig av vSphere Client på en Windows-dator eller så kan man använda sig av webbgränssnittet vSphere Web. (VMware, Inc. 2011d)

3.5 VMware vSphere Client

VMware vSphere Client är ett hanteringsverktyg som möjliggör hantering och kontroll av värddatorer och deras virtuella maskiner. VMware vSphere Client kan kopplas direkt till ESXi-värdatorn via IP-adress eller till vCenter Server genom IP-adress och portnummer (Figur 7). Om man kopplar direkt till en ESXi-värd kan man endast kontrollera de virtuella maskiner som finns där. Ifall man kopplar till verktyget vCenter Server kan man kontrollera flera olika ESXi-värdar och deras virtuella maskiner ifall de är anslutna till verktyget vCenter Server. Flera funktioner är tillgängliga ifall man kopplar till vCenter Server, t.ex. kloning och migration.



Figur 7. vSpheres olika användargränsnitt.

4 PROJEKTETS FÖRVERKLIGANDE

Detta kapitel beskriver de olika lösningarna som utarbetades för att förverkliga projektet. De olika metoderna demonstreras med exempel, samt motiveringar varför metoden fungerar eller varför inte. De huvudsakliga metoderna som användes var applikationsvirtualisering och full virtualisering.

4.1 Kriterier för val av programvara

Det används ungefär 200 olika program för underhåll och övervakning av komponenter i energibolagets automationssystem. Programmen som har använts i detta projekt är valda på basen av användarantal. Vilka program som är de mest använda har jag fått reda på genom diskussioner med automations- och elmontörer. Under projektets gång har åtta program testats. Genom att ha testat dessa program med olika virtualiseringsmöjligheter har jag kunnat visa på vilka/vilket sätt konceptet är möjligt (eller inte möjligt).

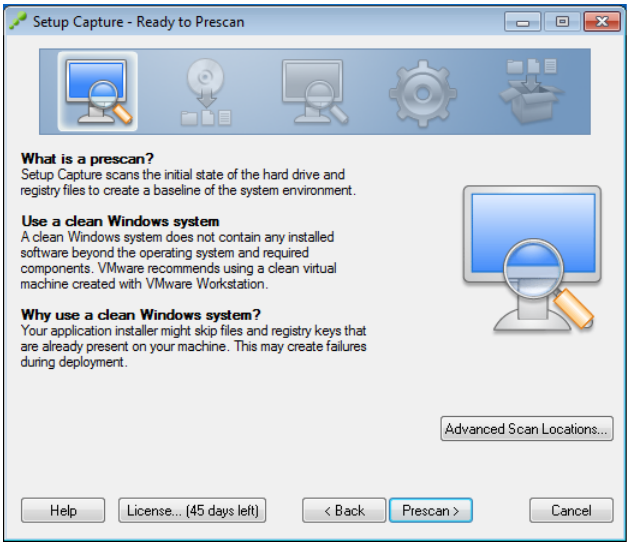
4.2 Applikationsvirtualisering

För att testa applikationsvirtualiseringsmetoden använde jag VMware ThinApp som presenteras i verktygkapitlet. Installation av ThinApp kräver registrering på VMwares hemsida. Licenskoden kommer per e-post till den e-postadress som gavs vid registreringstillfället. Jag har använt mig av en 60 dagars testlicens. Det rekommenderas att man installerar ThinApp på ett nyinstallerat operativsystem för att undvika onödiga filer i det slutliga paketet. Med hjälp av VMware Workstation skapade jag en virtuell dator med en ren Windows-installation. Sedan installerades ThinApp på den virtuella datorn.

Idén bakom detta koncept är att man skall kunna distribuera applikationer till datorer via nätet eller USB-sticka. När applikationen virtualiseras går den att starta var som helst. Efter att man har använt applikationen skall man kunna ta data tillvara. Som slutresultat skall man kunna köra applikationer var som helst t.ex. från en USB-sticka oberoende av underliggande operativsystem.

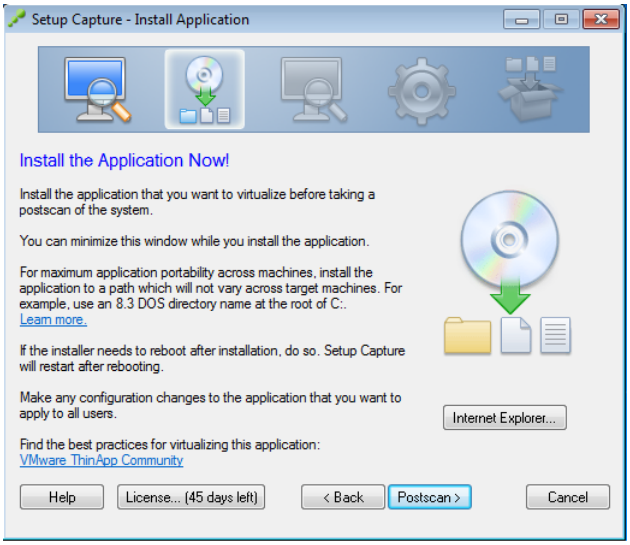
4.2.1 Skapa programpaket

Första steget kallas förskanning (prescan) och då går programmet igenom hårdskivan och registerfilerna för att skapa en helhetsbild av systemet. En ren Windows-installation rekommenderas för att göra hela processen snabbare. Ifall onödiga program är installerade kommer processen att räcka längre (Figur 8).



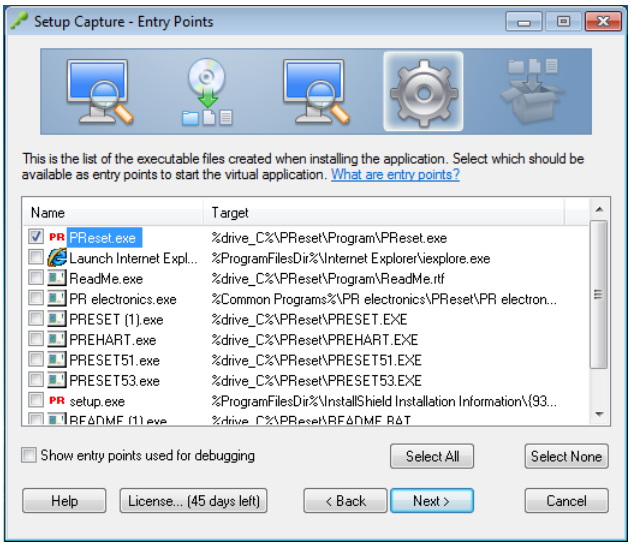
Figur 8. Förskanning.

Efter förskanningen begär programmet att man skall installera det program som man vill virtualisera. Programmet bör konfigureras nu för att man inte senare behöver konfigurera det vid varje uppstart. Programmet bör installeras på en sådan plats som inte varierar mellan operativsystem. (Figur 9).



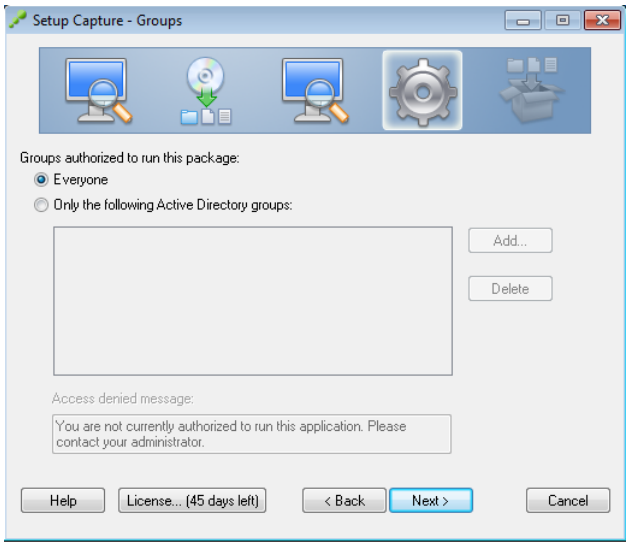
Figur 9. Installera programmet.

När programmet är installerat och konfigurerat börjar man efterskanningen (postscan). Efterskanningen skannar hela systemet på samma sätt som i förskanningen och jämför sedan resultaten med varandra. Efter efterskanningen visar programmet en lista på vad som ändrats sedan förskanningen. Nästa steg är att välja det installerade programmets exekverbara fil (Figur 10).



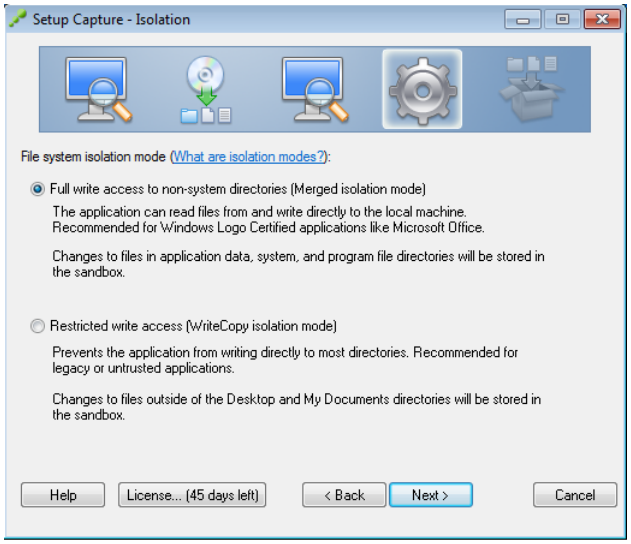
Figur 10. Efter efterskanningen.

Följande steg är användarrättigheterna. Man kan tillägga en grupp eller användare direkt från Active Directory ifall man bestämt sig att begränsa användarrättigheter. Ifall man installerar eller använder programmet via minnessticka bör alla ha rättigheter och då väljer man ”Everyone” (Figur 11).



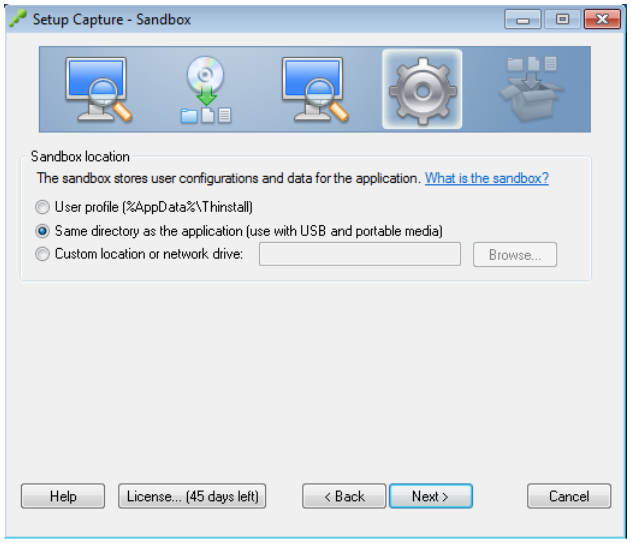
Figur 11. Användarrättigheter.

Efter användarrättigheterna väljer man själva virtualiserade programmets rättigheter. ”Merged isolation mode” ger rättigheter till programmet att läsa och skriva direkt på den lokala datorns hårdskiva. ”WriteCopy isolation mode” hindrar programmet från att skriva direkt på hårdskivan (Figur 12).



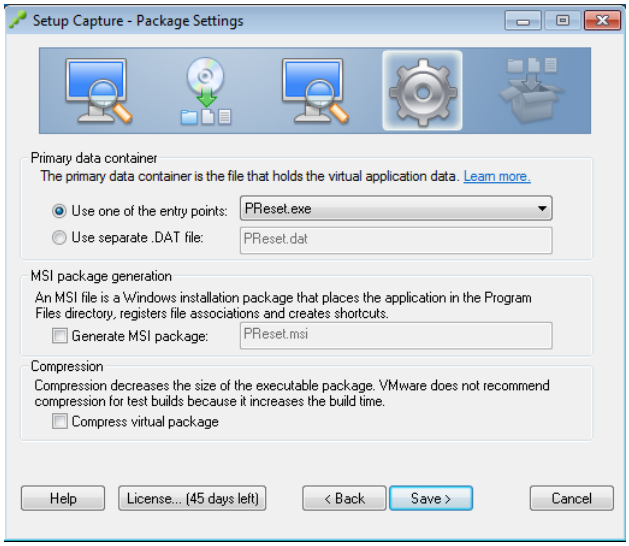
Figur 12. Programmets rättigheter.

Nästa steg är att välja en lagringsplats för alla ändringar som gjorts i programmet. Denna lagringsplats kallas sandlåda (sandbox). Sandlådan innehåller allting som behövs för att köra programmet, såsom nödvändiga mappar, registerfiler och inställningar (Figur 13). Var själva programpaketet lagras efter att det har skapats väljer man i nästa steg.



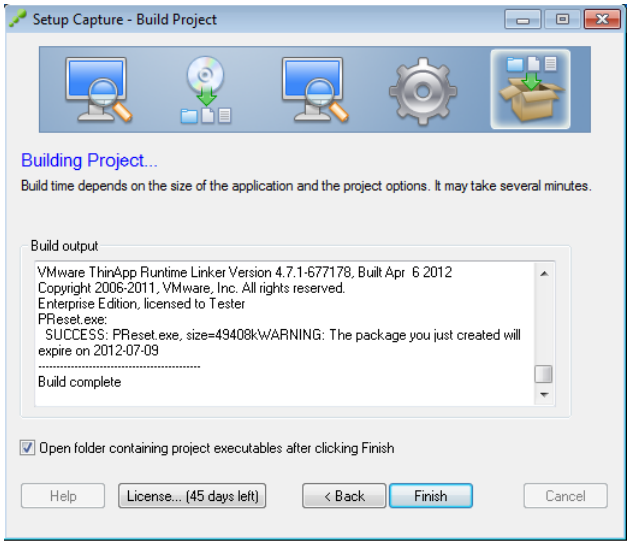
Figur 13. Val av lagringsplats.

Sedan väljer man paketets inställningar. Ifall programmet är tillräckligt litet föreslår ThinApp att programmets data kan sparas i samma fil. Om programmet är för stort föreslår ThinApp en .DAT fil för lagring av programdata. I det här skedet kan man också skapa en MSI-fil (Microsoft Installer) som gör det möjligt att installera programpaketet på samma sätt som ett vanligt ovirtualiserat program. Det är också möjligt att komprimera data ifall det är nödvändigt (Figur 14).



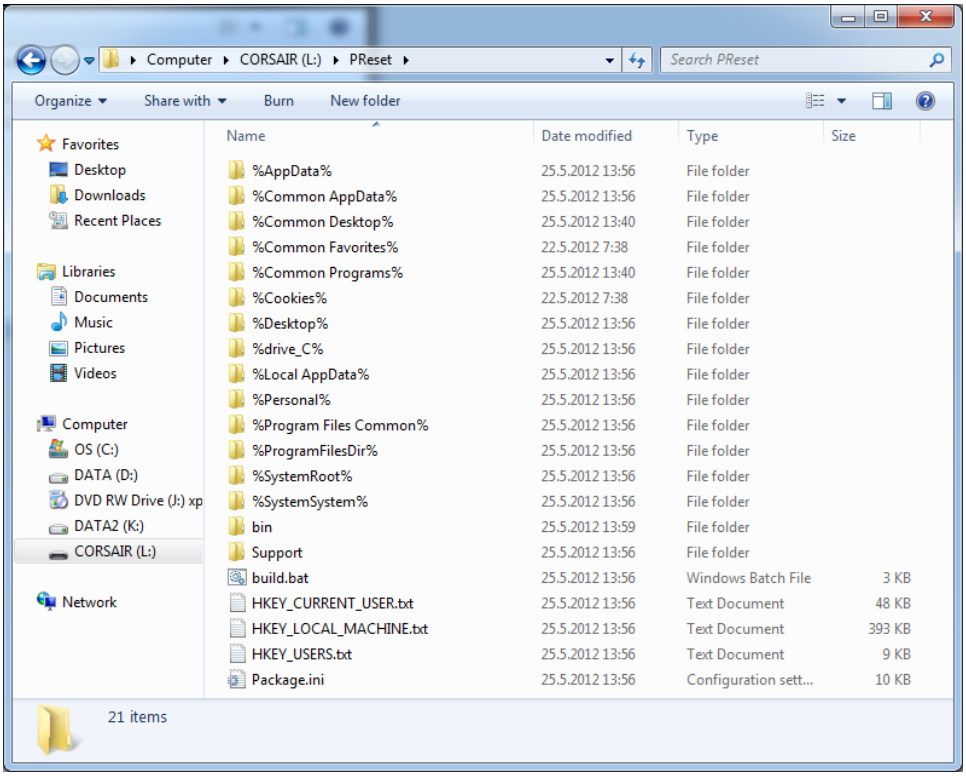
Figur 14. Paketinställningar.

I följande fönster kan användaren manuellt konfigurera programpaketets filer ifall det är nödvändigt. Det rekommenderas att man inte skall göra det. Efter det byggs programpaketet. Programpaketet fungerar så länge som ThinApp-licenskoden är i kraft.

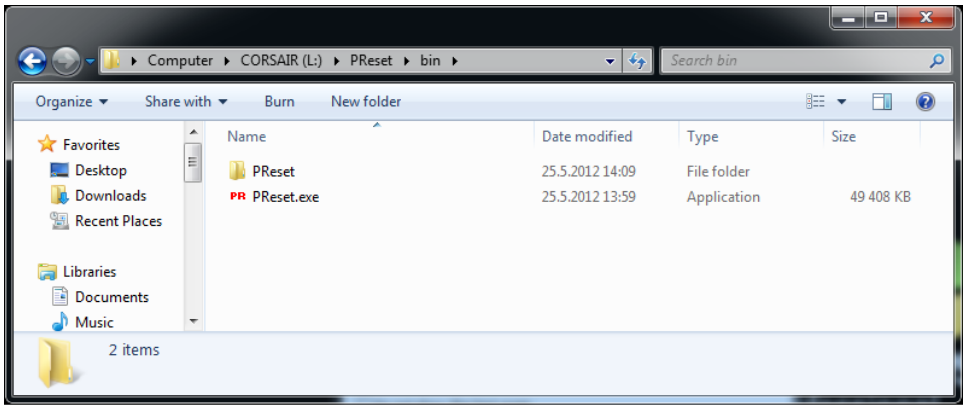


Figur 15. Programpaketet är färdigt.

Programpaketets filer finns där jag valde att de skulle sparas. Mappen som innehåller paketets filer är den så kallade sandlådan (Figur 16). Inne i bin-mappen ligger den exekverbara filen (Figur 17).



Figur 16. Sandlådan.

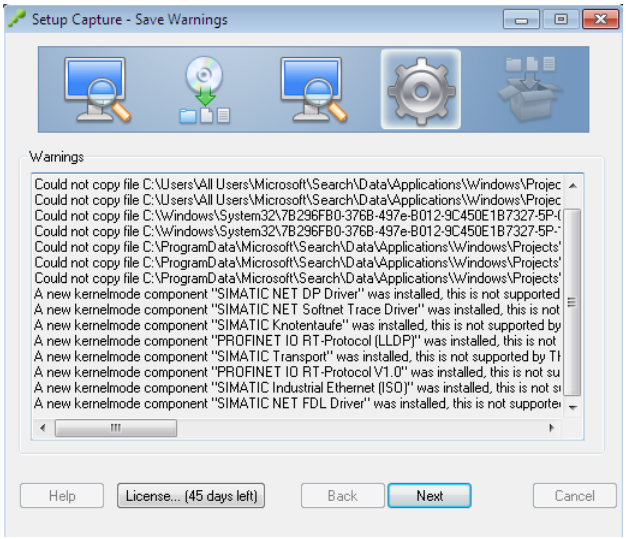


Figur 17. Exekverbara filen.

4.2.2 Problem

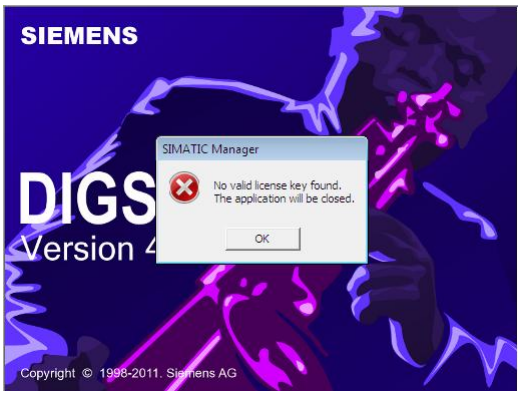
Det uppstod problem då jag testade Siemens-programvaror. Första problemet uppstod redan när programpaketet skapades med ThinApp. ThinApp meddelade att det inte går att kopiera åtta filer samt att åtta Siemens drivrutiner inte stöds av ThinApp. Trots

meddelandet kunde man fortsätta med att skapa programpaketet. De drivrutiner och filer som blev utomstående kunde ha kunnat skapa problem då man ansluter en komponent till datorn (Figur 18).



Figur 18. ThinApp felmeddelande.

Efter att ThinApp skapat programpaketet försökte jag starta Siemens-programmet DIGSI 4.84, men det gick inte för att ingen giltig licenskod hittades (Figur 19).



Figur 19. Licensproblem med Digsi 4.84.

Siemens-programvaror använder ett licensprogram, Automation License Manager (ALM), som startas som en process i bakgrunden av Windows. ALM sköter om de olika licenskoderna och berättar för Siemens-programvarorna om de är i kraft. Efter att man har gjort ett programpaket av ett Siemens-program med ThinApp uppstår det problem med licenserna. Orsaken bakom problemet är att ThinApp ändrar på den traditionella sökvägen och därför kan inte ALM-processen startas i bakgrunden. Sökte på webben om någon annan råkat ut för samma fel, men hittade inga relaterade diskussioner.

4.2.3 Resultat

Programpaketen som skapades före Siemens-programpaketen startade normalt. Deras användning testades dock aldrig eftersom konceptet inte fungerade med alla program. Eftersom programpaketens användning inte testades vet man inte vilka problem som kan ha uppstått. Ett problem som man troligtvis skulle ha stött på är kommunikationsproblem mellan den virtualiserade applikationen och serie- eller USB-porten. Som jag tidigare nämnde orsakade Siemens-programpaketen problem redan vid uppstart. Siemens-programpaketens komplikationer var orsaken till beslutet att slopa applikationsvirtualiseringsmetoden.

4.3 Full virtualisering

För att testa full virtualisering har jag använt programmet VMware Workstation 8.0 och 6.5 för att skapa virtuella testdatorer. Jag skapade också en liten infrastruktur för att kunna spara virtuella datorerna externt och för att underlätta deras underhåll. För att skapa infrastrukturen använde jag VMware vSphere Hypervisor (ESXi), VMware vCenter Server och VMware vSphere Client. Verktygen presenteras i verktygskapitlet. För att kunna installera VMware vCenter Server satte jag upp en Windows Server 2008 R2 64-bit.

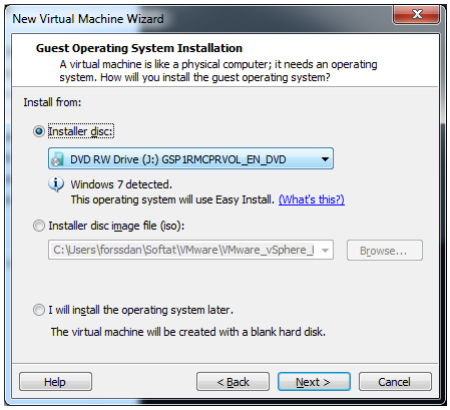
Idén bakom detta koncept är att man skall kunna köra processkomponenternas programvaror i virtuella datorer på en fysisk bärbar dator. Efter användning skall processkomponenternas programvarors data från den virtuella maskinen sparas externt och den fysiska bärbara datorn skall återställas.

4.3.1 Skapa en virtuell dator

Att skapa en virtuell dator med VMware Workstations ”New Virtual Machine Wizard” är smidigt och snabbt. Först steget är att välja mellan ”Typical” och ”Custom”. Jag väljer ”Typical” för att jag behöver inte göra specialinställningar (Figur 20).

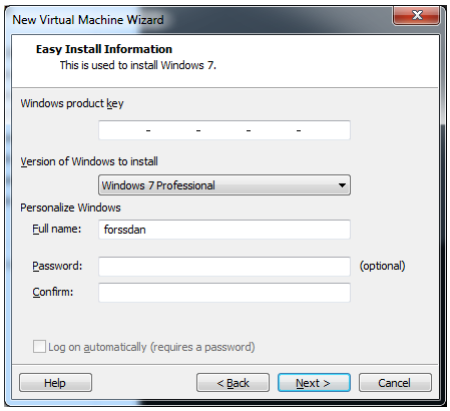
Figur 20. ”New Virtual Machine Wizard”.

I följande steg hittar skapningsprocessen automatiskt Windows-installationsmediet och berättar att ”Easy Install” kommer att användas (Figur 21).



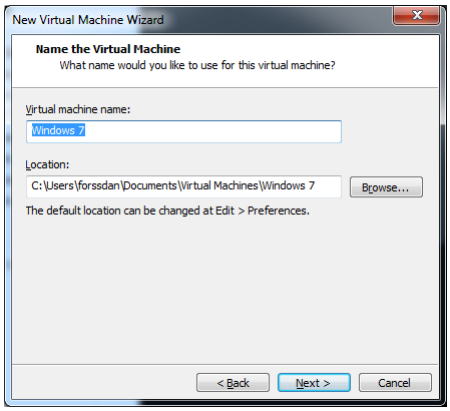
Figur 21. Installation av gäst operativsystemet.

”Easy Install” begär Windows-information för att göra installationen snabbare (Figur 22).



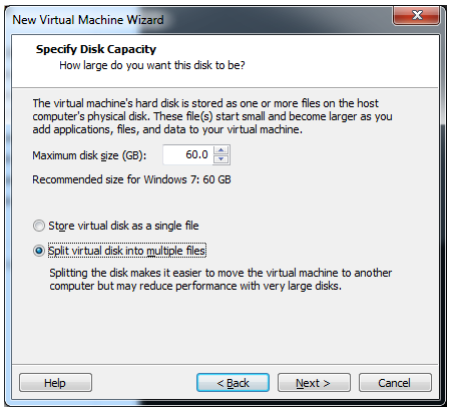
Figur 22. "Easy Install".

I nästa steg kan man definiera den virtuella maskinens namn samt var den skall sparas (Figur 23). Var virtuella maskinen sparas har ingen betydelse för att det går senare att flytta den eller ladda upp den till en värddator.



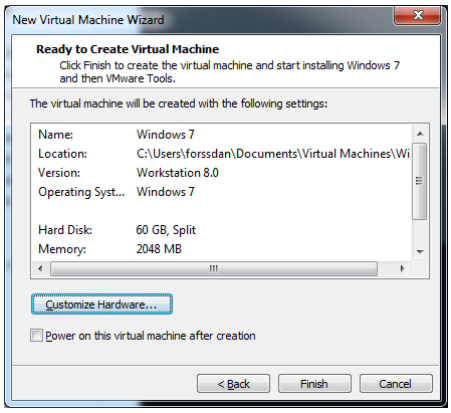
Figur 23. Namnge virtuella datorn.

I följande steg väljer man storleken på den virtuella hårdskivan. Oftast räcker den rekommenderade storleken. Ifall man kommer att flytta eller kopiera den virtuella datorn lönar det sig att välja ”Split virtual disk into multiple files” (Figur 24).



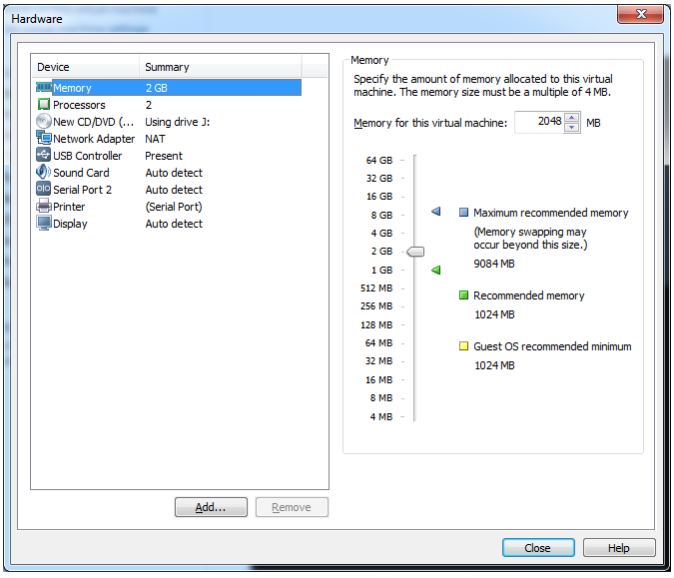
Figur 24. Virtuella hårdskivans storlek.

Förrän man skapar den virtuella maskinen kan man ännu göra inställningar gällande dess hårdvara via ”Customize Hardware” (Figur 25). Sedan installeras operativsystemet på samma sätt som på en fysisk dator.



Figur 25. Möjlighet att ändra på hårdvaran.

I ”Customize Hardware”-fönstret kan man ändra på hårdvaruinställningarna. Det är också möjligt att ändra på inställningarna efter att den virtuella maskinen är skapad. Man bör åtminstone ge rekommenderad mängd minne åt virtuella maskinen (Figur 26).



Figur 26. "Customize Hardware".

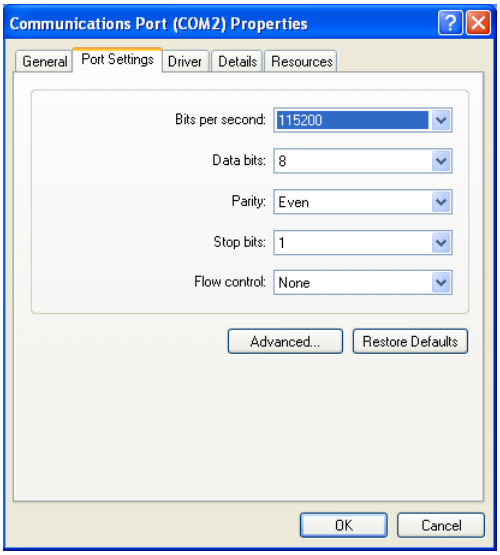
4.3.2 Testning och resultat

För att starta upp virtuella maskinerna på underhållsdatorn har jag använt mig av VMware Player 4.0.3 som kan skapa, starta och stoppa virtuella maskiner samt ändra på inställningarna. VMware Player är en förenklad version av Workstation.

Testandet utfördes tillsammans med en automations- eller elmontör. Orsaken var den att jag inte visste hur processkomponenternas programvaror fungerar och behövde därför

montörernas hjälp. Efter att ha testat programmen fick jag kunskap om hur de virtuella maskinerna skall konfigureras för att kunna kontakta processkomponenterna och på så sätt underhålla dem. Mera om inställningarna beskrivs i konfigurationskapitlet.

De flesta program kontaktar processkomponenterna via serieporten. Ibland måste man ändra på serieportens inställningar i Windows-enhetshanteraren (”Device Manager”). Till exempel en viss Siemens-processkomponent hade överföringshastigheten 115200 bit/s och pariteten ”Even”. Serieportarnas standardöverföringshastighet är 9600 bit/s och pariteten ”None”. Därför måste jag ändra inställningarna i den virtuella maskinens enhetshanterare innan jag kunde kontakta processkomponenten med programmet DIGSI 4.84 (Figur 27).



Figur 27. Serieportinställningar.

MaxLoader programmet kontaktar processkomponenten via en printerport. Den bärbara datormodellen som är tänkt att fungera som underhållsdator saknar printerport. Med hjälp av en USB-printerportkonverter var det dock möjligt att kontakta komponenten.

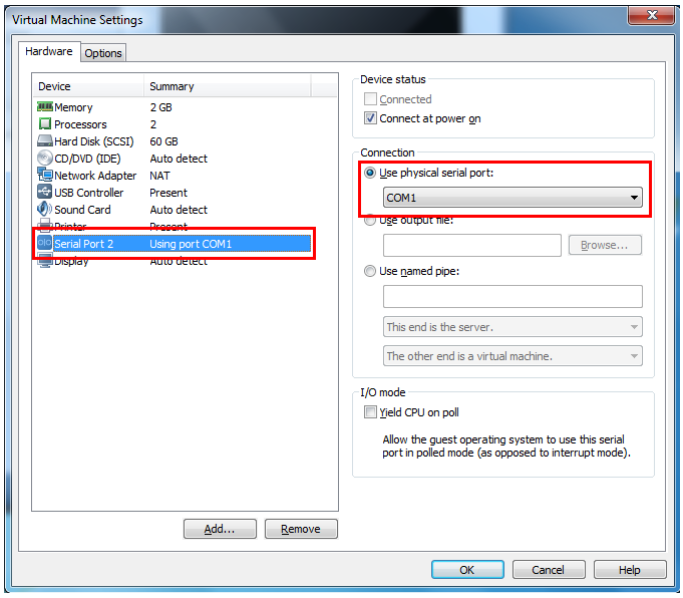
Programmet DIGSI 4.84 är ett versionskänsligt program. DIGSI 4.84 fungerade inte med den nya ”Workstation 8.0”-versionens virtuella maskiner. Problemet var att kontakten mellan datorn och komponenten brast av någon okänd orsak. Efter att ha kontaktat Siemens gällande problemet fick jag en förklaring varför det inte fungerar. Förklaringen var att DIGSI 4.84 inte stöder de nyaste virtualiseringsverktygen. Siemens tekniska support beskrev en miljö där programmet fungerar. Den virtuella datorn skall

skapas med Workstation 6.5 och köra Windows XP Professional Service Pack 3 som operativsystem. Efter att jag skapat miljön testade jag på nytt och jag kunde kontakta processkomponenten många gånger utan problem.

De andra programmen var inte versionskänsliga. Några program kunde endast installeras på operativsystemet Windows XP men fungerade även med Workstation 8.0 virtuella maskiner. Det uppstod några andra små problem. Enligt montörerna uppstår samma problem då man använder sig av en fysisk maskin. Därför kan man konstatera att virtualiseringsmetoden fungerar.

4.3.3 Konfigurering

Innan man startar den virtuella maskinen för första gången skall man konfigurera serieportens inställningar. Man skall använda alternativet som använder den fysiska maskinens serieport, ”COM 1”. Den fysiska serieporten ”COM 1” identifieras i den virtuella maskinen som serieport ”COM 2” (Figur 27).



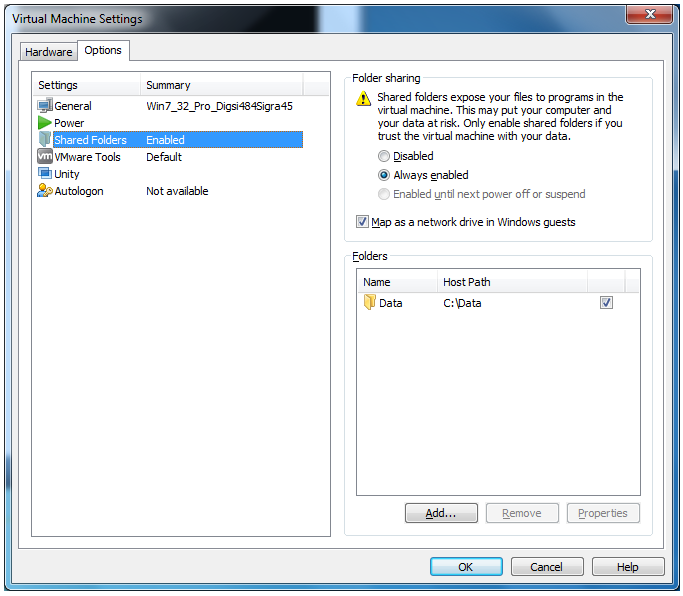
Figur 28. Konfigurering av serieport.

Den virtuella maskinens operativsystem, Windows, är konfigurerat så att det vid uppstart startar processkomponentens programvara automatiskt via startup. Windows-skrivbordet är tomt och inga andra programvaror är installerade. Användaren har möjlighet att spara programdata på en USB-sticka. Annars går det inte att göra någonting annat på den virtuella maskinen emedan den är härdad med ”Group Policy”.

Den virtuella maskinens datasäkerhet är till största delen under kontroll tack vare härdning med hjälp av ”Group Policy”. Som anti-virus program har jag installerat Symantec Endpoint Protection (SEP) som lämpar sig för virtuella datorer. Energibolaget använder programmet på de flesta maskiner för att det uppfyller säkerhetskraven. SEP är inställt så att det kontrollerar varje fil som kopieras, flyttas eller exekveras. Till exempel om man försöker köra ett program som är infekterat via en USB-sticka, berättar SEP för användaren att programmet är skadligt och kan därför inte startas.

4.3.4 Dataöverföring

Ett problem som skulle lösas var att ta reda på om det är möjligt att få data som processkomponentens programvara skapat flyttat till underhållsdatorns fysiska hårdskiva. I fönstret ”Virtual Machine Settings” under fliken ”Options” finns möjligheten att ge den virtuella maskinen tillgång till en mapp från den fysiska datorn (Figur 28). Mappen syns som en nätverksenhet i den virtuella maskinen. Den här inställningen görs också innan man startar virtuella maskinen första gången.

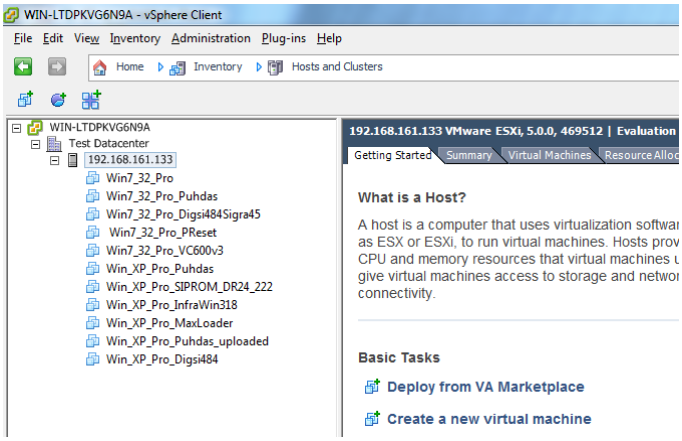


Figur 29. "Virtual Machine Settings".

Nästa steg var att starta upp virtuella maskinen och ställa in processkomponentens programvara. De program som skapar mätningsdata eller annan data, inställs så att de sparar data på den fysiska maskinen genom att spara allting på virtuella maskinens nätverksenhet.

4.3.5 Underhåll och lagring

Som jag tidigare nämnde har jag satt upp liten infrastruktur som kör VMware vSphere Hypervisor (ESXi) och VMware vCenter Server. VMware vCenter Server är installerad på Windows Server 2008 R2 64-bit. Virtuella maskinerna är skapade med VMware Workstation 8.0 eller 6.5 och har senare blivit uppladdade för lagring till ESXi-värden med Workstations ”Upload”-verktyg. Fördelen med att ha alla virtuella maskinerna på ESXi-värden är att man kommer åt dem på distans genom att kontakta ESXi-värden med VMware vSphere Client (Figur 30).



Figur 30. VMware vSphere Client.

När nya program skall installeras börjar man med att klona en virtuell maskin som har en ren Windows-installation. Man namnger den enligt programnamnet och sedan installerar man den nya programvaran. Efter att allting är installerat laddar man ner den virtuella maskinen från infrastrukturen och konfigurerar den.

En annan fördel är att man behöver uppdatera endast den virtuella maskin som ligger i ESXi-värden. Sedan kopierar man den uppdaterade virtuella maskinen till den fysiska underhållsdatorn. Det lönar sig att göra en säkerhetsplan eller ett schema som man följer för att undvika risken att man glömmer att uppdatera virusskyddet och systemet.

4.4 Underhållsdatorn

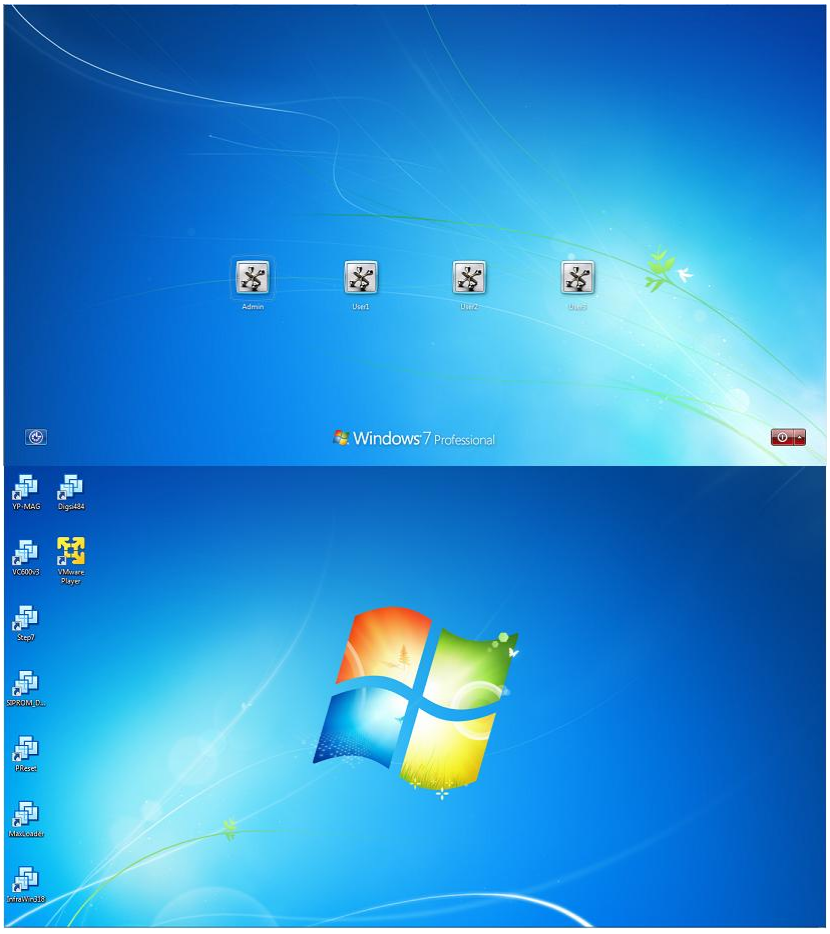
Underhållsdatorn exekverar Windows 7 Professional 64-bit för att kunna utnyttja 8 Gb minne. Det är viktigt att den fysiska datorn har mycket minne för att virtualiseringsmjukvaran skall kunna fungera optimalt. Underhållsdatorn är försedd med USB-portar och en serieport. Det är också möjligt att docka maskinen till en

dockningsstation. Maskinen är avsedd för fältbruk. Den bärbara dator som är tänkt att fungera som underhållsdator är Panasonic Toughbook CF-53. En teknisk specifikation finns som bilaga.

4.4.1 Härdning och säkerhet

Underhållsdatorns användare skall endast kunna starta virtuella maskiner. Det skall inte vara möjligt att starta andra program eller tjänster förutom på administratorns profil. För att uppnå dessa krav är Windows härdat med ”Group Policy”.

I Windows-inloggningsmenyn har varje avdelning ett eget användarnamn. Varje användarnamn har ett eget skrivbord med endast de virtuella maskiner som är installerade med avdelningens program (Figur 31). Den virtuella maskinen startas med användarnamnet och sedan startas programmet automatiskt då den virtuella maskinen har startat Windows.



Figur 31. Inloggningsmenyn och skrivbordet.

Som anti-virus program har jag installerat Symantec Endpoint Protection (SEP) som också lämpar sig för dessa datorer. Som jag tidigare nämnde i kapitlet 4.3.3 använder energibolaget SEP-programmet på de flesta maskiner för att det uppfyller säkerhetskraven. SEP är inställt så att det kontrollerar varje fil som kopieras, flyttas eller exekveras.

5 DISKUSSION OCH SLUTSATSER

I detta arbete har jag genom testning kunnat visa att det är möjligt att skapa en miljö för processkomponenternas programvaror. Miljön är lätt att underhålla och datasäkerheten är på en tillräckligt hög nivå. Jag har fått kunskap om virtualisering och en bra bild av hur infrastrukturer är uppställda. Jag har testat två olika virtualiseringsmetoder, applikations- och full virtualisering.

Det uppstod licensproblem då Siemens-programvarorna gjordes till virtuella applikationer. Energibolaget använder många Siemens-programvaror och samma licensproblem skulle ha uppstått med dem också. På grund av detta testresultat gjordes beslutet att applikationsvirtualisering inte fungerar för detta ändamål.

Den andra virtualiseringsmetoden som jag testade var full virtualisering. Den här metoden orsakade också problem. Problemen kunde dock lösas efter samarbete med Siemens. Det är bra att veta att processkomponenternas programvaror kan vara versionskänsliga eller operativsystemskänsliga. Eftersom full virtualisering fungerar trots versionsproblemen och går att upprätthålla har jag inte testat flera miljömöjligheter. Istället undersökte jag hur man skulle kunna utveckla konceptet.

5.1 Vidareutveckling

Trots att konceptet fungerar och data från komponenternas programvaror går att spara på den fysiska maskinen kommer det att kräva vidareutveckling. Efter att alla inställningar och konfigurationer gjorts på den fysiska maskinen kan man ta en ren kopia av den. Efter att en montör har använt datorn hämtar han den tillbaka till en dockningsstation. När datorn kopplas till dockningsstationen skall data som processkomponenternas programvara har skapat sparas externt i en infrastruktur. Efter att data har laddats upp hämtas kopian av den rena installationen till den fysiska datorns hårdskiva. På det här sättet minskar risken att virus eller annat skadligt program kommer åt infrastrukturen eller processkomponenten.

Fortum har redan fungerande infrastrukturer som kan användas till detta ändamål. Problemet är hur data skall flyttas från den fysiska maskinen till infrastrukturen och hur skall den rena kopian flyttas till den fysiska maskinen. Infrastrukturen bör automatiskt identifiera när en dator ansluts och sedan utföra dataöverföringen. Alla datorer skall vara bärbara och helst av samma modell för att konceptet skall fungera.

KÄLLOR

Burford David. *2008,* Virtualization - Is it right for you [www].
Tillgänglig: http://www.ladenterprizes.com/pdf/Virtualization.pdf Hämtad 16.4.2012

Citrix Systems, Inc. 2011, Desktop virtualization and security: a global market research report [www], publicerad 2011.
Tillgänglig:
http://www.citrix.com/site/resources/dynamic/additional/Security_Index_Whitepaper.pdf Hämtad 16.4.2012

Dijk Liz van. 2008, Application virtualization [www], publicerad 25.2.2008
Tillgänglig: http://www.it.anandtech.com/show/2456/2 Hämtad 2.5.2012

Elmsjö Henrik. 2012, Så härdar du din virtuella miljö – 7 steg till ökad säkerhet, Techworld [www], publicerad 10.1.2012
Tillgänglig: http://www.idg.se/2.1085/1.424924/sa-hardar-du-din-virtuella-miljo--7-steg-till-okad-sakerhet/sida/4/7-skapa-sakra-virtuella-switchar Hämtad 25.4.2012

Hoefer C.N & Karagiannis G. 2010, Taxonomy of cloud computing services, *IEEE Globecom 2010 Workshop on Enabling the Future Service-Oriented Interne*, s. 1345-1350.

Hämäläinen Pertti. 2007, Verkkovoimaa virtuaalisesti, *Tietokone*, nr 13/2007, s. 61.

InfoBarrel. 2010, History of Virtualization [www], publicerad 2010.
Tillgänglig: http://www.infobarrel.com/History_of_Virtualization Hämtad 17.4.2012

Murugesan San. 2008, Harnessing Green IT: Principles and Practices, *IT Professional* volym 10, nr 1, s. 24-33.

Mäntylä Juha-Matti. *2008,* Virtualisointi mullistaa tietotekniikan [www], publicerad 30.11.2008.
Tillgänglig:
http://www.tietoviikko.fi/cio/virtualisointi+mullistaa+tietotekniikan/a192316
Hämtad 16.4.2012

Ribière Alain. 2008, Using virtualization to improve durability and portability of industrial applications, *Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on*, s. 1545-1550.

Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Zhuolin Yang, Jianyong Chen. 2011, Virtualization security for cloud computing service, *2011 International Conference on Cloud and Service Computing,* s. 174-179

Solomon Michael.G. 2010, *Security Strategies in Windows Platforms and Applications*, Jones & Bartlett Learning, 400 s.

Strickland, Jonathan. 2008, How Server Virtualization Works [www]. Tillgänglig: http://computer.howstuffworks.com/server-virtualization2.htm Hämtad 7.5.2012

VMware, Inc. 2011a, VMware ThinApp – Application Virtualization Made Simple [www] Tillgänglig: http://www.vmware.com/files/pdf/thinapp/VMware-ThinApp-Datasheet.pdf Hämtad 21.5.2012

VMware, Inc. 2011b, VMware Workstation 8 – Your On-Ramp to the Cloud [www] Tillgänglig: http://www.vmware.com/files/pdf/VMware-Workstation-Datasheet.pdf Hämtad 21.5.2012

VMware, Inc. 2011c, VMware vSphere: Install, Configure, Manage, Student Manual – Volume 1, 368 s.

VMware, Inc. 2011d, VMware vCenter Server – Unify and Simplify Virtualization Management [www] Tillgänglig: http://www.vmware.com/files/pdf/products/vCenter/VMware-vCenter-Server-Datasheet.pdf Hämtad 21.5.2012

BILAGA: MOBILE BUSINESS EXCELLENCE

Panasonic recommends Windows® 7.

MOBILE BUSINESS EXCELLENCE

The CF-53 is equipped with a second-generation Intel® Core™ i5 platform and Genuine Windows 7 Professional. Designed for all mobile professionals, including small and medium-sized business users, looking for outstanding value and mission-critical application access, it represents core Toughbook benefits combined with semi-rugged protection.

Mobile Computing Platform	Intel® Core™ i5-2520M vPro™ processor (2.5GHz, 3MB Intel® Smart Cache, Intel® 6 series Express chipset QM67)	
Operating System	Genuine Windows® 7 Professional	
RAM	4GB DDR3 SDRAM (max. 8GB)	
Graphic Chip	Intel® HD Graphics 3000, UMA (Windows® 7 64 bit max. 1696MB, 32bit max. 1428MB)	
Storage	320GB (SATA)	
CD/DVD Drive	DVD Super MULTI Drive	
LCD	14" Active Matrix (TFT) colour LCD 1366 x 768 pixels (HD)	
Bluetooth™	2.1 + EDR Class 1	
Wireless LAN	Intel® Centrino® Advanced-N 6205 AGN WLAN	
	IEEE 802.11 a/b/g/n compliant; slide on/off switch	
LAN	IEEE 802.3 10Base-T / IEEE 802.3u 100BASE-TX / IEEE 802.3ab 1000BASE-T (2nd LAN Project based)	
Modem	Data: 56 kbps (V.92) FAX: 14.4 kbps (Project based)	
Sound	WAVE and MIDI playback, Intel® High Definition Audio subsystem support	
Security	TPM (TCG V1.2 compliant) Password security (supervisor password, user password, hard disc lock) Integrated hardware security lock slot	
Card Slots	PC Card Slot*	x 1, Type I or Type II, Allowable current 3.3 V: 400 mA, 5 V: 400 mA
	ExpressCard Slot*	x 1, ExpressCard/34 or ExpressCard/54
	SD/SDXC Memory card slot	x 1
	RAM Module Slot	x 2, DDR3 SDRAM, 204-pin, 1.5 V, SO-DIMM, PC3-10600 Compliant, one slot occupied
Interfaces	Serial (16550A compatible)	Dsub, 9-pin
	VGA	Mini Dsub, 15-pin
	HDMI	x 1
	Headphones	Mini-jack, 3.5 DIA, stereo
	Microphone	Mini-jack, 3.5 DIA, stereo
	DC input	Jack
	USB 2.0	x 3, 4-pin
	USB 3.0	x 1, 4-pin
	Firewire (IEEE1394a)	x 1, 4-pin (Project based)
	Modem	RJ-11 (Project based)
	LAN	RJ-45 (2nd LAN Project based)
	Port replicator	100-pin
Keyboard / Pointing Device	88 keys / Touch Pad	
Power	AC Adaptor	Input: 100V ~ 240V, 50Hz/60Hz; Output: 15.6V, 7.05A
	Battery	Lithium-Ion (10.8V, Typical 6750 mAh / Minimum 6300 mAh)
	Battery life	Approx. 10h (Mobile Mark™ 2007, LCD brightness: 60cd/m²)
	Power Management	Standby function, ACPI BIOS
Dimensions (W x H x D)	341mm x 48-55mm x 281mm/13.6" x 1.9 - 2.2" x 11.2" (including carrying handle)	
Weight	Approx. 2.65 kg /5.84 lb (including carrying handle)	
Webcam (optional)	1.3 Mpx with digital microphone	
Integrated Options	Fingerprint Reader, Smart Card Reader, 3G Mobile Broadband (HSPA+, up to 21Mbps)	
Accessories	AC Adaptor	CF-AA5713A
	Battery charger	CF-VCBTB2W
	Battery pack	CF-VZSU71U ("road warrior" 9 cell, 73Wh)
		CF-VZSU46AU ("road warrior" 9 cell, 92Wh)
	Port replicator	CF-VEB531U

* Config. A: 1x PC Card Type I or II + 1x ExpressCard - Config. B: 2x PC Card Type I or II, no ExpressCard

As an ENERGY STAR® Partner, Panasonic Corporation has determined that this product meets the ENERGY STAR® guidelines for energy efficiency. Active Matrix colour display conforms to industry standards. Some displays may contain isolated illuminated or dark pixels as an artefact of the manufacturing process (effective pixels: minimum 99.998%). RAM capacity calculated as follows: 1MB = 1,048,576 bytes. HDD capacity calculated as follows: 1GB = 1,000,000,000 bytes. Toughbook is a brand name and registered trademark of Panasonic Corporation. Acrobat® is a registered trademark of Adobe® Systems Incorporated. Intel, the Intel logo, Intel Core, Intel vPro, Core Inside and vPro Inside are trademarks of Intel Corporation in the U.S. and other countries. Microsoft® and Windows® are registered trademarks of Microsoft® Corporation of the United States and/or other countries. All other brand names shown are the registered trademarks of the relevant companies. All rights reserved. All working conditions, times and figures quoted are optimum or ideal levels and may differ as a result of individual and local circumstances. Panasonic Marketing Europe GmbH, Panasonic Computer Products Europe Headquarters, Hagenauer Straße 43, 65203 Wiesbaden (Germany).

Panasonic
ideas for life